Liebesschwindel im Cyberspace – aktuelle Forschungsergebnisse zum Phänomen des Romance Scam im Überblick

Christian Thiel

1. Einführung

„Wenn sich der Traummann als Betrüger entpuppt“[1], „Im Netz des falschen Traumprinzen“[2] oder „Wenn Sehnsucht blind macht“[3] – mit diesen Schlagzeilen berichteten Zeitungen über den Fall einer verwitweten Rentnerin, die im Internet einen angeblichen US-Soldaten kennengelernt und ihm – ohne ihn jemals gesehen zu haben – ihr gesamtes Erspartes überwiesen hat. Sie hatte bereits einen Kredit von mehr als 40.000 Euro beantragt, als ein Mitarbeiter der Bank misstrauisch wurde und die Polizei einschaltete. Diese eröffnete der Frau, dass sie Opfer eines ‚Romantikbetrugs‘ geworden ist.

Dieser in der medialen Darstellung unglaublich erscheinende Betrug ist kein Einzelfall. Allein das Landeskriminalamt Baden-Württemberg hat innerhalb des Jahres 2017 ganze 131 solcher Fälle erfasst[4]. Die Dunkelziffer ist vermutlich um ein Vielfaches höher, denn schließlich lohnt sich diese Betrugsmasche: Die Summen, um die Romantikbetrüger ihre Opfer schädigen, sind häufig exorbitant hoch – der Schaden kann in die Hunderttausende gehen.

Der Romantikbetrug ist grundsätzlich ein recht neues Phänomen der Internetkriminalität, weswegen nur wenige Erkenntnisse hierzu vorliegen. Ziel dieses Beitrags ist es, einen systematischen Überblick der bisherigen Forschungsergebnisse zum Romantikbetrug zusammenzustellen. Auf Grundlage der internationalen Literatur aus Kriminologie, Psychologie und Soziologie wird das Phänomen zunächst dargestellt und verortet (Abschnitt 2) und dann der typische Verlauf nachgezeichnet (Abschnitt 3). Es folgen Erkenntnisse über die Täter (Abschnitt 4) und die Geschädigten (Abschnitt 5). Abschließend werden diverse Erklärungsansätze hinsichtlich der Wirkungsweise dieser Betrugsart vorgestellt (Abschnitt Kapitel 6).

2. Das Phänomen Romantikbetrug

2.1. Hintergrund: Dating und Täuschung in der virtuellen Welt

Der Romantikbetrug – obgleich keineswegs eine ‚Erfindung‘ des Internetzeitalters (vgl. Abschnitt 4) – muss vor dem Hintergrund der durch das Internet angestoßenen gesellschaftlichen Veränderungen betrachtet werden. Einer der Bereiche des alltäglichen Lebens, den das Inter-

1 Berliner Kurier, 27. November 2017, S. 38.

2 Frankfurter Rundschau, 27. November 2017, S. 34.

3 Frankfurter Presse, 27. November 2017, Echo Vermischtes, S. 1.

4 Frankfurter Rundschau, 27. November 2017, S. 34.

net fundamental verändert, ist der der Liebe und Sexualität (Kaufmann 2011). So ist beispielsweise das seit einigen Jahren boomende ‚Online-Dating' mittlerweile zu einer gesellschaftlich breit akzeptierten Form der Kontaktanbahnung intimer Beziehungen geworden (Aretz et al. 2017). Dabei ist ein äußerst lukrativer Markt mit hohen Teilnehmer- und Umsatzzahlen entstanden, der jedoch auch Gefahren beinhaltet. Zu diesen gehören neben unseriösen Geschäftspraktiken (Abofallen etc.) und Datenschutzproblemen auch Manipulationen und *Täuschungen* diverser Akteure – von bezahlten Animateuren (sog. IKM-Schreibern[5]) über Trolle und Stalker bis hin zu „malware writers and scammers" (Arora und Scheiber 2017, S. 414).

Grundsätzlich ist Täuschung ein allgegenwärtiges Element in der Online-Welt. Vor allem bei der Selbstdarstellung im Bereich der virtuellen Partnersuche wird getrickst und geschummelt, so werden etwa Angaben (etwa zu Gewicht, Größe, Verdienst etc.) geschönt oder Bilder durch allerlei Kniffe ‚optimiert'. Allerdings gibt es hierbei – im Normalfall – ein mäßigendes Korrektiv, und zwar die Antizipation eines Face-to-Face-Treffens (Toma 2017, S. 425). Das Online-Dating spaltet nämlich die Begegnung in zwei Phasen – das initiale Kennenlernen online und das anschließende Treffen im ‚richtigen' Leben. Zwischen diesen beiden Phasen gibt es einen „Brucheffekt" (Kaufmann 2011, S. 17), denn das erste reale Treffen ist keine bloße Fortsetzung des Onlinekontakts. Die sich treffenden Individuen sind in verschiedener Hinsicht ‚anders', als sie im Netz waren – schon weil sie jetzt physisch in Erscheinung treten. Wenn dabei die reale Erscheinung zu sehr von der Online-Inszenierung abweicht, sprich hemmungslos getäuscht wurde, gilt dies als „relational deal-breaker" (Toma 2017, S. 425). Die Täuschungen in der virtuellen Selbstpräsentation müssen also in einem „konventionell akzeptablen Maß" (Zillmann et al. 2011, S. 312) bleiben, da eine zu große ‚Ent-Täuschung' beim ersten realen Treffen die Chance auf eine Beziehung deutlich verringern würde. Die meisten Menschen gehen also beim Online-Dating davon aus, dass die Selbstdarstellungen ihres Gegenübers wahrscheinlich geschönt, jedoch nicht komplett erfunden sind. Gleichzeitig versuchen sie beständig, die Vertrauenswürdigkeit des anderen über dessen Kommunikationsverhalten einzuschätzen. Dies gibt ihnen eine gewisse Sicherheit, die allerdings – wie Studien zeigen – eine trügerische ist. Denn „people tend to rely on the wrong cues" (Toma 2017, S. 426). Sie achten primär auf Signale, die entweder gar nichts über die tatsächliche Vertrauenswürdigkeit aussagen oder leicht in betrügerischer Absicht kopiert werden können. Kurz zusammengefasst: Viele Menschen gehen in der virtuellen Welt davon aus, dass Täuschungen *erstens* meist auf ein geringes Maß beschränkt bleiben und *zweitens* relativ sicher von ihnen erkannt werden können. Diese Überzeugungen erweisen sich beim Romantikbetrug, aber auch

[5] Der Begriff , Internet-Kontaktmarkt'-Schreiber bezeichnet Personen, die gegen Bezahlung virtuelle Identitäten im Internet (v.a. auf Singlebörsen und Social Media) einnehmen. Dies dient dazu, andere Teilnehmer zu einer fortgesetzten Teilnahme am Portal oder zu Inanspruchnahme kostenpflichtiger Dienste zu motivieren und ihnen teilweise auch unlautere oder betrügerische Angebote zu unterbreiten.

bei vielen anderen Delikten aus dem Bereich der Internetkriminalität, als gefährlicher Trugschluss.

2.2. Definition und Prävalenz des Romantikbetrugs

Der Romantikbetrug (im Folgenden als „IRS“ abgekürzt[6]) kann definiert werden als eine Betrugsform, bei der Kriminelle mittels falscher Identitäten (Profile) und über onlinebasierte Kommunikation (Dating-Seiten, Messenger, Soziale Medien etc.) strategisch ein Vertrauensverhältnis zu einem Opfer anbahnen, dabei eine romantische Beziehung vortäuschen und das Opfer derart in emotionale Abhängigkeit verstricken, dass es dem Täter für vorgebliche Gründe teils hohe Geldsummen zukommen lässt.

Der IRS beinhaltet Elemente mehrerer teils alter Betrugspraktiken (Heiratsschwindel, Identitätsdiebstahl, Massenmarketing-Betrug), die neu kombiniert wurden und sich zudem die Eigenheiten des Internetzeitalters zunutze machen (Buchanan und Whitty 2014, S. 262; Marx und Rüdiger 2017, S. 211; Whitty 2013, S. 667). Es handelt sich dabei allerdings keineswegs um eine simple Masche, die nur bei naiven und gefühlsduseligen Personen Wirkung zeigt, sondern um einen „advanced, sophisticated and therefore very dangerous type of scam” (Kopp et al. 2016, S. 148).

Nicht selten wird der IRS in der medialen Berichterstattung aufgrund angenommener Wesensverwandtschaft (das ‚Ausnutzen von Liebe‘) oder ähnlicher Modi Operandi gemeinsam mit weiteren Delikten abgehandelt. Dabei drohen jedoch charakteristische Merkmale – das typische Vorgehen, die charakteristischen Opfer- und Tätergruppen usw. – aus dem Blick zu geraten. Vom IRS abzugrenzende Delikte sind *im Internet* etwa „Sextortion“ (eine Erpressungsmethode mit kompromittierendem Bildmaterial), „Cybergrooming“ (eine Art des onlinebasierten sexuellen Missbrauchs von Kindern; vgl. Rüdiger 2012) oder „Realfakes“/„Catfishing“ (eine komplexe Identitätstäuschung mit dem Ziel der emotional-psychischen Manipulation der Betroffenen; vgl. Schwartz 2015); *in der Realwelt* gibt es (immer noch) den „klassischen Heiratsschwindel“, auch in einer modernisierten, globalisierten Form als „Bezness“ (junge Liebesbetrüger vorwiegend aus den Maghreb-Ländern gehen zum Zwecke der finanziellen Ausbeutung Beziehungen/Ehen mit westlichen Touristinnen ein).

Leider existieren zum Delikt „IRS“ bisher kaum belastbare Zahlen. In Deutschland wird diese Betrugsform nicht separat in der Polizeilichen Kriminalstatistik (PKS) aufgeführt, sondern wie viele andere Betrugsdelikte unter der Sammelkategorie „sonstige weitere Betrugsarten“ (518900) subsumiert. In anderen Ländern gibt es zumindest einige Statistiken. In den

6 Der Romantikbetrug firmiert unter einer ganzen Reihe an Begrifflichkeiten: Romance Scam (bzw. Scamming), Love Scam, Sweetheart Scam, Online Dating Scam, Liebesbetrug oder Online-Heiratsschwindel. Inzwischen ist auch in der deutschen Kriminalistik die englische Bezeichnung „Romance Scam“ üblich. Das Akronym „IRS“ (für: Internet Romance Scam) soll die Wiederholung unschöner Anglizismen vermeiden und grenzt die Deliktform deutlicher von realweltlichen Heiratsschwindeleien und Romantikbetrügereien ab.

USA rangiert der IRS laut „Internet Crime Complaint Center (IC3)“[7] seit 2016 unter den Top 3 (nach Schadenshöhe) der zur Anzeige gebrachten Internetverbrechen. 2017 haben sich in den USA über 15.000 Betroffene gemeldet, von denen 57 % einen Vermögensschaden erlitten haben. Dieser summierte sich auf über 211 Millionen US$. In *Australien* erreichten die Regierungsorganisation „Scamwatch“[8] im Jahr 2017 über 3.000 Meldungen, davon 23,5 % vollendete Taten mit einem Gesamtschaden von über 20 Millionen AU$. Auch in *England*[9] zählt der IRS zu den häufigsten Betrugsarten (Action Fraud listet ihn unter den „Top 8 Scams“ für 2018[10]). Hier wurden im Jahr 2016 3.889 Opfer um insgesamt £39 Millionen betrogen[11]. Der Royal Canadian Mounted Police in *Kanada* wurden im Jahr 2016 1.142 Fälle von IRS angezeigt, davon 770 vollendete Taten mit einem Gesamtschaden von mehr als 18 Millionen CAD[12]. Alles in allem lassen sich aufgrund der mangelhaften Datenlage, die durch die dem IRS immanente enorme Dunkelziffer (vgl. Füllgrabe 2015) zusätzlich verzerrt wird, keine belastbaren Aussagen zu regionaler Häufigkeit/Verbreitung, Viktimisierungsquoten, Prävalenzraten usw. treffen. Mit einiger Vorsicht lässt sich jedoch Folgendes ableiten: Es scheint, dass der IRS ein relativ neues Phänomen ist, das erstmals um 2007 herum in den Blick der Strafverfolgungsbehörden rückte (Whitty und Buchanan 2012). Die Fallzahlen und damit auch die Schadenssummen sind seither kontinuierlich, teilweise sogar drastisch gestiegen. Insgesamt ist von relativ hohen Geschädigtenzahlen und großen Schadenssummen auszugehen.

3. Typischer Verlauf des Romantikbetrugs

Der IRS folgt in der Praxis häufig einem sehr schematischen Ablauf. Verschiedene Studien haben diese Ablaufmuster herausgearbeitet und in unterschiedliche Phasen unterteilt (etwa Marx und Rüdiger 2017, S. 213; Whitty 2013, S. 677–679). Der vorliegende Beitrag schlägt

7 Das IC3 ist eine 2001 gegründete Arbeitsgruppe des Federal Bureau of Investigation (FBI), des National White Collar Crime Center (NW3C) und des Bureau of Justice Assistance (BJA). Es bietet Opfern von Cyberkriminalität die Möglichkeit, unkompliziert Delikte zu melden. Die „Annual Reports“ finden sich unter https://www.ic3.gov/media/annualreports.aspx [28.03.2018].

8 Scamwatch wird betrieben von der Regierungsbehörde „Australian Competition and Consumer Commission (ACCC)“. Statistiken finden sich unter https://www.scamwatch.gov.au/about-scamwatch/scam-statistics [28.03.2018].

9 Das „National Fraud Intelligence Bureau (NFIB)“ ist eine an die Metropolitan Police London angegliederte Polizeidienststelle, die Informationen zu Betrug und finanziell motivierter Cyberkriminalität sammelt und auswertet. Die von ihr betriebene Einrichtung „Action Fraud“ (https://www.actionfraud.police.uk) dient als Meldestelle für Betrugsopfer und als Informationsschnittstelle für die Öffentlichkeit.

10 https://www.actionfraud.police.uk/news/the-top-8-frauds-to-watch-out-for-in-2018 [28.03.2018]

11 http://www.bbc.com/news/uk-38678089 [28.03.2018]

12 http://www.rcmp.gc.ca/en/gazette/romance-scams?fe [28.03.2018]

ein etwas abgewandeltes Modell vor, bei dem folgende Phasen unterschieden werden: Ködern – Vertrauen aufbauen – Vermögen abschöpfen – Reviktimisieren.

3.1. Die Phase des Köderns

Der erste Schritt für die Täter ist es, ein fiktives *Profil*, also eine initiale Selbstpräsentation, zu erstellen, die zumeist aus Angaben wie Name, Nationalität, Alter, Beruf, Hobbies, Lebenseinstellungen sowie einigen Fotos besteht. Dieser Profilerstellung kommt im Cyberspace allgemein eine tragende strategische Bedeutung zu. Schließlich bestimmt die Art und Weise der hier durchgeführten Selbstdarstellung im Wesentlichen das Ausmaß der Aufmerksamkeits- und Kontaktchancen und somit die Wahrscheinlichkeit, dass ein Nutzer in der Masse der Profile überhaupt wahrgenommen und positiv beurteilt wird. Wichtig ist dabei v.a. eines: Da die – gerade dem Online-Dating inhärente – Selbstdarstellung mittels Texten und Fotos eine Art einseitiges Kommunikationsangebot an potentielle Profilbetrachter darstellt, darf sie – will das Profil erfolgreich sein – nicht einfach individuelle Besonderheiten abbilden, sondern muss die Darstellung in erster Linie an die Erwartungen der anderen anschlussfähig machen. Anders formuliert: Es geht nicht um individuelle Einmaligkeit, sondern um eine Einordnung in verschiedene soziale Bewertungskategorien. Eine Ausrichtung am ‚common sense' hinsichtlich Attraktivität, Geschlechterrollen, Interessen und sozioökonomischem Status ist hier ausgesprochen wichtig. Dies wiederum ermöglicht Betrügern, die ja nicht der o.g. ‚Bremse' eines möglichen Face-to-Face-Treffens unterliegen, ein geradezu ‚über-ideales' Profil zu gestalten. Typische Profile sind etwa:

- *Der männliche Scammer*: Der Betrüger präsentiert sich als gutaussehender Mann zwischen 40 und 60 Jahren, der beruflich als Geschäftsmann, Manager oder hochrangiger Militärangehöriger[13] tätig ist, kurzum einen hohen sozioökonomischen Status innehat. Er beschreibt sich als wohlhabend, loyal, respektvoll, humorvoll, religiös sowie maskulin. Sofern Hobbys genannt werden, besteht kein Interesse an typischen ‚Männer-Aktivitäten' (wie etwa Fußball), sondern an Tätigkeiten wie Fitness, Kochen oder Tanzen. Zumeist hat er eine tragische Lebenssituation hinter sich (Tod der Ehefrau, des Kindes, der Eltern; schwierige Scheidung usw.) und sucht nun eine liebende Frau (Füllgrabe 2015; Kopp et al. 2015; Whitty 2013, 2015). Als Nationalität geben die in Deutschland agierenden Betrüger meist englischsprachige Länder an (USA, England, Australien), womit sie auch ihre schlechten Deutschkenntnisse erklären[14]. In den englischsprachigen Ländern wird hingegen häufig die Nationalität der Opfer vorgetäuscht.
- *Der weibliche Scammer*: Fake-Frauen sind deutlich jünger als ihre männlichen Pendants (meist nicht älter als 30) und äußerlich ausgesprochen attraktiv. Sie sind finanziell unabhängig, aber nicht wohlhabend; meist haben sie schlecht bezahlte Jobs als Krankenschwestern, Lehrerin, Studentin oder Verkäuferin. Ihre Hobbys entsprechen gängigen

13 Diese Legende ist derart typisch, dass sie auch als „Military Scam" bekannt geworden ist.

14 Laut kriminalpolizeilicher Einschätzung sind rund 95 % der Englisch sprechenden Kontakte auf deutschen Dating-Seiten Romance-Scammer. Es gibt allerdings auch etliche, die perfekt Deutsch sprechen. https://www.polizei-beratung.de/themen-und-tipps/betrug/scamming/rat-und-hilfe/ [letzter Zugriff: 18.04.2018]

> Gender-Stereotypen (Musik, Fitness, Sport; selten auch ungewöhnlichere Aktivitäten wie Motorsport oder Fußball). Sie sind nicht an Geld interessiert, selbstbewusst und suchen die ‚wahre Liebe', was sexuelle Anzüglichkeiten nicht ausschließt. Mit dem nicht selten erheblichen Altersunterschied zu den (männlichen) Opfern haben sie selbstredend kein Problem (Füllgrabe 2015; Kopp et al. 2015; Whitty 2013, 2015). Die vorgegebenen Nationalitäten variieren hier mehr als bei den Fake-Männern, nicht selten werden sogar die wahren Herkunftsländer angegeben[15] .

Weiterhin wird auch von homosexuellen Profilen berichtet, wobei diese noch keine so große Verbreitung gefunden zu haben scheinen oder aber eine noch höheren Dunkelziffer aufweisen.

Das Profil ist quasi der ‚Köder' und die Betrüger versuchen diesen so zu gestalten, dass er für ihre Opfer möglichst attraktiv ist. Sie greifen dazu verbreitete, stereotype Annahmen über Partnerwünsche von Frauen und Männern (z.B. Frauen suchen Partner mit hohem sozioökonomischen Status, Männer achten eher auf physische Attraktivität[16]) auf und bedienen diese durch entsprechende Fotos[17] und Angaben, die meist eher vage gehalten sind, wodurch sie es dem Opfer ermöglichen, die ‚Leerstellen' mit den eigenen Wünschen und Hoffnungen aufzufüllen (Füllgrabe 2015, S. 488; Whitty 2013, S. 677). Natürlich ist auch ein attraktiv und überzeugend gestaltetes Profil kein Selbstläufer; in einem bestimmten situativen Kontext jedoch – also eben beispielsweise auf einer Dating-Seite, deren Mitglieder stark motiviert sind, ihren idealen Partner zu finden (Whitty 2013, S. 677) – kann es einen starken Effekt haben.

Grundsätzlich stecken die Betrüger in den Aufbau der Profile viel Arbeit; wahrscheinlich testen sie auch, welche Arten von Profilen am erfolgreichsten sind. Die Angaben in den Profilen (Beruf, Fotos, Hobbys und Interessen) dienen dabei nicht nur der Präsentation eines idealen Partners, sondern geben gleichzeitig subtile Hinweise für die weitere Entwicklung der Betrugsnarration.

---

15 Der Russian Dating Scam ist eine (kriminalistischen Einschätzungen zufolge nicht mehr so verbreitete) Variante des IRS, die sich vom hier behandelten IRS v.a. hinsichtlich der dahinterstehenden Tätergruppierungen unterscheidet. Die zumeist russischstämmigen Betrüger posieren dabei als gutaussehende Frauen auf Partnersuche. Als Wohnort wird zumeist Russland (insbesondere Cheboksary, Kasan, Moskau, Luhans'k) angegeben – wohl, weil dort der Mittelpunkt des betrügerischen Netzwerkes angesiedelt ist (Heubrock und Böttcher 2011, S. 79).

16 Darin spiegeln sich auch typische asymmetrische Mechanismen der Partnerwahl: Frauen präferieren eher Männer mit hoher Bildung und Einkommen; Männer sind auch gewillt, sich mit vergleichsweise niedriger gebildeten und einkommensschwachen Frauen zu treffen (Aretz et al. 2017, S. 19–20).

17 Die von den Scammern verwendeten Fotos (sehr attraktiver Menschen) sind in den meisten Fällen gestohlen oder einfach von den Social-Media-Auftritten der jeweiligen Personen kopiert. Einige dieser zu Täuschungszwecken missbrauchten Bilder zieren inzwischen Hunderte von gefälschten Profilen. Gerade Bilderserien von einer Person sind für Scammer interessant, denn sie können damit dem Opfer immer wieder fotographische ‚Beweise' ihrer Existenz schicken.

Mit dem erstellten Profil kontaktieren die Täter ausgewählte Opfer. Nach welchen Kriterien sie ihre Auswahl treffen, ist nicht bekannt und lässt sich allenfalls aus einer Typologisierung der Opfer ableiten (die natürlich durch die Dunkelziffer verzerrt ist). In den vergangenen Jahren erfolgte die Kontaktaufnahme zu den Opfern v.a. über Dating-Portale oder Soziale Medien (v.a. Facebook), inzwischen oft auch direkt über Fotos-Apps (v.a. Instagram) (Marx und Rüdiger 2017, S. 212). Auch direkte Ansprachen via Messenger und E-Mail kommen vor; die Adressen recherchieren die Täter aus dem Netz oder beziehen sie über teils dubiose Adresshändler.

Unabhängig vom Kontaktkanal gestaltet sich die Kontaktaufnahme immer gleich: Ein kurzes „Hallo“, gefolgt von einer Einladung zum Chatten, der dann – sofern diese angenommen wird – die Selbstpräsentation des Betrügers (das Profil sowie einige ansprechende Fotos) folgt. Die anschließende Kommunikation erfolgt teils in Englisch, teils auch in Deutsch, wobei dann ein Computerübersetzungsprogramm (google translator) genutzt wird. An den dadurch entstehenden oft radebrechenden Formulierungen („Honig ich werde Sie zahlen zurück mit Interesse“) stören sich nur die wenigsten Opfer. Falls der Kontakt über ein Dating-Portal zustande gekommen ist, leiten die Betrüger ihre Opfer kurz nach dem ersten Kontakt auf direkte Kommunikationskanäle (wie Messenger oder Email) um. Dadurch machen sie sich von der Partnerbörse unabhängig und laufen nicht Gefahr, durch Entlarvung und Sperrung seitens des Administrators den Kontakt zu den Opfern zu verlieren (Heubrock und Böttcher 2011, S. 77). Denn nicht selten werden die Fake-Profile nach dem ‚Abfischen‘ der Mail-Adressen bereits nach wenigen Tagen gelöscht: entweder durch den Administrator, sofern dieser den Account als Scammer identifiziert hat, oder durch den Scammer selbst, der damit vermeidet, dass sein Opfer die Korrespondenz mit den Profilangaben abgleicht und dabei möglicherweise Widersprüche aufdeckt (Heubrock und Böttcher 2011, S. 78).

3.2. Die Phase des Vertrauensaufbaus

In dieser auch „Grooming“ (Whitty 2013) genannten Phase wickeln‘ die Täter das Opfer ein. Sie erschleichen sein/ihr Vertrauen, indem sie eine scheinbar sichere Umgebung schaffen, in der das Opfer seine intimsten Gedanken, Geheimnisse und Unsicherheiten erzählen kann. Dies funktioniert gerade über computervermittelte Kommunikation sehr gut. Das Fehlen nonverbaler Signale bei der computervermittelten Kommunikation führt nämlich – wie der Kommunikationswissenschaftler Joseph Walther in seinem „hyperpersonal model“ (Walther 1996) beschreibt – dazu, dass mehr persönliche Informationen ausgetauscht werden als in der Face-to-Face-Kommunikation. Solche hyperpersonellen Kommunikationen erscheinen manchen attraktiver als Face-to-Face-Kommunikationen, da sie die Möglichkeit bieten, einem idealisierten (und sich selbst idealisierenden) Gegenüber in einem scheinbar geschützten und unsichtbaren Raum das tiefste Innere zu offenbaren. Die rein auf die Nachricht beschränkte selektive Selbstdarstellung, die aufgrund der Asynchronität der Kommunikation obendrein

optimierbar ist, kann leicht zu einer Idealisierung des Kommunikationspartners führen. Dieser Effekt verstärkt sich noch, indem die Betrüger ihre Kommunikation auf ihr jeweiliges Opfer zuschneiden. Durch geschicktes Fragen und genaues Zuhören finden die Betrüger heraus, welche Vorstellung einer idealen Beziehung bzw. eines idealen Partners das Opfer hat, die sie dann entsprechend bedienen. Auffällig ist ferner, dass die meisten Betrüger das Opfer sehr schnell mit Kosenamen ansprechen, ihm die Liebe erklären und das Bild einer gemeinsamen Zukunft aufbauen (Füllgrabe 2015). Hierbei kommt eine Fülle an schwülstig-poetischen Liebeserklärungen und Komplimenten zum Einsatz, bei denen die Scammer zumeist auf vorgefertigte Skripte zurückgreifen. Diese bausteinartigen Liebesschwüre sowie das regelmäßig geheuchelte Interesse („wie war dein Tag?“) sind sozusagen das Minimalprogramm, das in vielen Fällen schon ausreicht. Versiertere Betrüger geben darüber hinaus auch noch vermeintlich private Details aus ihrem fiktiven Leben preis – sie erzählen von ihren Kindern, ihrem Beruf, ihren Problemen, Hoffnungen und Wünschen. Damit entlocken sie ihrem Opfer reziprok intime Details über sein/ihr Leben, die sie wiederum geschickt in ihre Betrugsnarrationen einflechten. Das Opfer erlebt dies als vermeintlichen Seelengleichklang und übersieht, dass die wahrgenommenen Gemeinsamkeiten – sei es der Musikgeschmack, die politischen Ansichten oder die Hobbys – nur aufgrund der eigenen Erzählungen oder der im Internet preisgegebenen Informationen konstruiert wurden[18].

Zusätzlich beschwichtigen die Scammer geschickt (und teilweise prospektiv) das vielleicht noch latent vorhandene Misstrauen. Unaufgefordert bestätigt der Betrüger seine Erzählungen, sei es durch die Übersendung von Fotos oder Dokumenten oder durch die Aussagen anderer Personen (vermeintliche Freunde, Familienangehörige, Rechtsanwälte, Diplomaten oder Ärzte). Manche Opfer bestehen in dieser Phase auf Telefonate oder gar Videochats. Die Betrüger wissen sich auch hier zu helfen: Telefonate werden mittels Follow-me-Mobiltelefonen oder über IP-Telefonie geführt, wodurch die Herkunft des Anrufenden verschleiert werden kann (so kann etwa ein Scammer aus Ghana mit einer britischen Vorwahl telefonieren). Bei Videochats (Skype) werden technische Probleme vorgeschoben, wegen derer die Kamera nicht verwendet werden können oder gestohlene Videos vorgespielt, während man aufgrund des ‚defekten‘ Mikrophons schriftlich kommuniziert.

Insgesamt hat dieses mal Tage, mal Monate dauernde ‚Grooming‘ für das Opfer folgende Konsequenzen: Es befindet sich nun in einer sehr intimen ‚Beziehung‘, die schon aufgrund der hohen Kommunikationsfrequenz (mehrere SMS, Mails, Chats pro Tag) einen großen Teil seines/ihres Alltag einnimmt. Mitunter resultiert daraus auch ein Stück weit Isolation vom gewohnten sozialen Umfeld, zumindest wenn dieses skeptisch oder kritisch darauf rea-

[18] Der ‚digitale Narzissmus‘, der einige Menschen eine Vielzahl an Informationen über ihr berufliches und privates Leben im Netz preisgeben lässt, macht es den Täter einfach, sich auf die spezifischen Bedürfnisse und Interesse ihrer Opfer einzustellen (Marx und Rüdiger 2017, S. 212).

giert, dass das Opfer eine derart tiefe Bindung zu einer Person hat, die keiner je gesehen hat, die aber gleichzeitig ‚zu toll um wahr zu sein' scheint[19]. An diesem Punkt fühlt sich das Opfer in einer sich entwickelnden Liebesgeschichte, die – den Versprechen des Betrügers zufolge – sehr bald in ein glückliches und finanziell abgesichertes, mitunter sogar luxuriöses Leben zu zweit münden soll.

3.3. Die Phase der Vermögensabschöpfung

Nachdem die Betrüger einige Zeit lang Vertrauen aufgebaut haben, kommt unweigerlich der für sie entscheidende Punkt: Sie bitten das Opfer um Geld. Um zu verhindern, dass die von ihnen sorgsam aufgebaute ‚Liebesgeschichte' durch die Geldforderung einen vorzeitigen Bruch erfährt, bereiten die Täter dies sorgsam vor (Kopp et al. 2015, S. 212). Von Beginn an entwickeln sie parallel zu der Liebesgeschichte eine zweite Narration – gewissermaßen das ‚Geld-Drama', indem sie subtil entsprechende Hinweise streuen und beide Erzählstränge anschließend so miteinander verflechten, dass das Geld zur Vorbedingung der Liebe, also der glücklichen gemeinsamen Zukunft, wird (Kopp et al. 2016). Die entsprechenden ‚Geld-Dramen' variieren stark, lassen sich aber in der Regel zwei großen Kategorien zuordnen: Krisen und Investments. *Krisengeschichten* thematisieren eine Notlage, in die der/die vermeintlich Zukünftige unverschuldet geraten ist und wegen der er/sie sich verzweifelt an das Opfer mit Bitte um finanzielle Hilfe wendet (geschäftliche Schwierigkeiten, Krankheit, Verhaftung etc.). *Investitionsgeschichten* wiederum stellen dem Opfer einen finanziellen Gewinn (bzw. ein gemeinsames Leben in Wohlstand) in Aussicht, zu dessen Erlangung allerdings vorab finanzielle Investitionen zu leisten sind (Schatzfund, Hausverkauf, Erlangung von Pensionsansprüchen etc.). Die Betrüger nutzen verschiedene Taktiken, die sie ggf. auch abwechseln oder kombinieren, um Geldforderungen in ihre Geschichten einzubetten – mal werden zur Überprüfung der Zahlungsbereitschaft des Opfers nur kleine Geschenke erbeten (Buchanan und Whitty 2014, S. 262), mal wird eine anfänglich kleine Unterstützung im Laufe einer eskalierenden ‚Krise' sukzessive erhöht, mal werden unmittelbar hohe Geldforderungen gestellt und bei Weigerung des Opfers schrittweise reduziert (Whitty 2013) und mal verlangen die Betrüger nur kleine Geldbeträge (Begleichen von Lebenshaltungskosten, Universitätsgebühren etc.), dies dafür aber regelmäßig und über mehrere Jahre (Füllgrabe 2015, S. 489).

Schlägt eine Taktik fehl und das Opfer weigert sich zu zahlen, wird zur Phase des Vertrauensaufbaus zurückgekehrt, um zu einem späteren Zeitpunkt erneut einen Versuch mit derselben oder einer anderen Taktik zu unternehmen (Whitty 2013, S. 679). Auf diese Weise

19 Diese Isolationstendenzen verstärken sich immens, sobald die erste Geldzahlung stattgefunden hat. Viele Opfer verheimlichen dann bewusst die Beziehung (zumindest den Teil mit dem Geld), schon um keine warnenden Hinweise signifikanter Anderer (v.a. Familie, Freunde) zu erhalten, die sie in kognitive Dissonanz versetzen würden.

werden die Geldüberweisungen auch aufrechterhalten. Auf einen erfolgten Geldtransfer folgt immer ein erneuter Vertrauensaufbau und dann wieder eine Geldforderung. Meist ist die Frequenz, in der Geld gefordert wird, sehr hoch und es liegen nur wenige Tage zwischen der angeblich ‚einmaligen' oder ‚garantiert letzten' Finanzspritze und dem erneuten Einfordern eines Betrags. Weigert sich das Opfer, bauen die Täter massiv Druck[20] auf – es wird gefleht, die baldige Rückzahlung mit Zinsen in Aussicht gestellt oder mit Beziehungsende, Gesamtverlust des bisher ‚geliehenen' Geldes oder gar Selbstmord gedroht. Häufig dramatisiert sich die Situation zunehmend – die ‚Krise' wird immer schlimmer und gleichzeitig rückt die Aussicht, den ‚Geliebten' bei sich zu haben, immer näher. Dieses ständige Schwanken zwischen emotionalen Extremen – Liebe und Wunscherfüllung einerseits, Druck und Angst andererseits – ist für die Opfer sehr belastend.

3.4. Die Phase der Reviktimisierung

Die Täter würden die Täuschung nie von sich aus auflösen, es sei denn, sie gründen einen erneuten Betrug darauf. Wie und wann können sich Opfer also aus der Täuschung befreien? Gemeinhin würde man vermuten, dass im Laufe des Betrugs der psychologische Druck bei den Opfern – allein schon durch das zunehmende Ausschöpfen der eigenen Geldquellen – derart zu- und die Plausibilität der ständigen Geldforderungen derart abnimmt, dass sie quasi automatisch zur Erkenntnis kommen, betrogen worden zu sein. Das scheint allerdings kaum der Fall zu sein. Es kommt zwar vor, dass Opfer durch eigene Zweifel und Recherchen der Täuschung auf die Schliche kommen und den Kontakt zu dem Betrüger abbrechen. Dies geschieht jedoch eher selten und wenn in frühen Phasen des Betrugs. Je mehr und je öfter ein Opfer Geld übereignet hat, desto tiefer ist es in die Täuschung verstrickt. In den meisten Fällen bedarf es deswegen eines Anstoßes durch Dritte, in erster Linie der Polizei (die etwa durch Bankmitarbeiter, besorgte Verwandte und Freunde oder im Rahmen einer Geldwäsche-Ermittlung auf den Fall aufmerksam wird). Doch selbst nachdrückliche Warnungen und das Vorlegen von Beweisen für die falsche Identität der Täter durch die Polizei stoßen bei vielen Opfern auf taube Ohren[21]. Denn die ‚Ent-Täuschung' vom Betrug ist emotional äußerst schmerzvoll. Viele Opfer haben gefühlt nicht nur Geld, sondern auch einen geliebten Menschen verloren. Sie leiden nach der Aufdeckung des Betrugs unter negativen Gefühlen wie Depression, Scham, Ärger, Furcht, Suizidgedanken usw. (Füllgrabe 2015, S. 490). Schon deswegen wollen viele mal mehr, mal weniger bewusst den Kontakt mit dem Betrüger nicht

20 So forderte etwa ein Betrüger seine ‚Verlobte' dazu auf, ihren 93-jährigen Erb-Onkel zu töten, mit der Begründung, dann könne man endlich eine schöne Hochzeit feiern (Nürnberger Nachrichten, Samstag 20. August 2016, Rubrik Stadt Nürnberg).

21 Mitunter geht die Verfangenheit in der Täuschung so weit, dass Opfer, die nicht wahrhaben wollen, dass hinter ihrem Traumpartner eigentlich kriminelle Organisationen stecken, nach Afrika fliegen, um sich auf die Suche nach diesem zu begeben. Dabei werden Fälle von Kidnapping und hohen Lösegeldforderungen berichtet.

ganz abbrechen. Häufig erfolgt dann eine *Reviktimisierung* bzw. eine „second wave of the scam" (Whitty und Buchanan 2016, S. 182), denn die Betrüger melden sich erneut, reaktivieren alte Gefühle und setzen dann entweder die alte Masche fort oder bringen neue Betrugsgeschichten in Anschlag. Opfern, die das Geld am meisten schmerzt, suggerieren die Täter beispielsweise, sie seien Polizisten, die – gegen Gebühr – das erbeutete Geld zurückbringen könnten. Bei jenen, die der verlorenen Liebe nachtrauern, meldet sich etwa ein Bestatter, der berichtet, der Partner wäre auf dem Weg zum Flughafen tödlich verunglückt und könne nur mit finanzieller Hilfe des Opfers eine würdige Bestattung erhalten. Oder aber der Scammer gibt schließlich ‚reumütig' zu, er sei ein Betrüger, doch habe er sich inzwischen in das Opfer verliebt (und brauche aber natürlich weiterhin Geld) (Whitty und Buchanan 2016, S. 185). Sollten die Geschädigten irgendwann definitiv kein Geld mehr haben bzw. auftreiben können, werden sie von den Betrügern nicht selten als Finanzagenten eingesetzt.

4. Täter und Täterwissen

Bisher liegen nur wenige Erkenntnisse über Täter und Täterwissen vor. Nach der Einschätzung vieler Ermittler sind die meisten IRS auf Täter aus Nigeria, Ghana und Kamerun zurückzuführen. Gleichzeitig handelt es sich beim IRS um ein globales Phänomen. Auch wenn der Schwerpunkt in Bezug auf die Opfer auf Australien, Europa und den USA zu liegen scheint, häufen sich in den letzten Jahren Berichte aus aller Welt, v.a. aus dem südostasiatischen Raum, aus Malaysia (Koon und Yoong 2013) und Indien (Arora und Scheiber 2017).

Der IRS kann dabei einer primär in Westafrika verorteten *Subkultur des Betrugs* zugerechnet werden, auf deren Konto auch andere typische Cybercrime-Delikte begehen (Boateng et al. 2011; Ellis 2016; Oduro-Frimpong 2014). Kriminalhistorisch erlebte diese ihre Initialzündung, als in den 1980er Jahren nigerianische Banden begannen – zunächst per Fax, später via E-Mail – hunderttausende Betrugs-Anschreiben in alle Welt zu versenden. Ihre bekannteste Masche, der ‚419 scam'[22], wurde zu einem globalen Massenphänomen und die dahinterstehenden Tätergruppierungen als ‚Nigeria Connection' berühmt-berüchtigt. Auch wenn diese Bezeichnung es nahelegt, handelt es sich hier nicht um eine strukturierte Organisation, sondern (zumindest derzeit noch) um viele kleine – teils unabhängige, teils lose verbundene – Gruppen. Diese verändern sich ständig und entwickeln auch ihre Modi Operandi weiter. Anstelle der klassischen langen und erzählerisch ausgeschmückten Nigeria-Mails treten heute

22 Die Masche lässt sich zwar unter dem Namen „spanish prisoner" bis ins 16. Jahrhundert zurückverfolgen Gillespie 2017, ist aber seit mehreren Jahrzehnten derart mit Nigeria verknüpft, dass sie nach dem § 419 (‚Betrug') des nigerianischen Strafgesetzbuchs benannt wurde. Das Grundprinzip ist, einer Person in einem Anschreiben ein großes Vermögen (Erbe, Lottogewinn, geheimes Konto etc.) in Aussicht zu stellen, davor jedoch verschiedene ‚Gebühren' (als Vorschuss) zu kassieren. Das Geld existiert natürlich nicht, die Vorschuss-Zahlungen können allerdings schnell exorbitante Höhen erreichen.

zunehmend Variationen und teils auch Kombinationen mit anderen Betrugsmaschen auf[23]. Eine derartige Weiterentwicklung ist auch der IRS, der das erste Mal 2007 in England aktenkundig wurde (Buchanan und Whitty 2014, S. 262)[24]. Seine Entwicklung hing v.a. damit zusammen, dass nigerianische Betrüger um die Jahrtausendwende ihre Betrugsaktivitäten nach Ghana verlagerten, wohl wegen des seit damals erhöhten Ermittlungsdrucks durch die nigerianische Finanzpolizei. Sie brachten ihr ‚Betrugswissen' mit, also jene „cyber-fraud paradigms or storylines that have proven economically fruitful when employed in the past" (Warner 2011, S. 743). Die lernwilligen ghanaischen Betrüger adaptierten diese und modifizierten Köder und Zielgruppe: die ‚Geschäftsbeziehung' beim 419 scam, mit der ein großes Vermögen erlangt werden soll, wurde beim IRS zu einer ‚Liebesbeziehung', die ein Happy End in Zweisamkeit (und Wohlstand) in Aussicht stellt.

Diese so entstandene ‚Masche' des Liebesbetrugs wurde (und wird) sukzessive verbessert und professionalisiert. So ist einer der Hauptschwachpunkte beim IRS der ‚Version 1.0', nämlich der direkte Bezug zu Afrika, inzwischen weitgehend eliminiert. Früher konnten Dating-Portale auffällige IP-Adressen aus Verdachtsländern einfach herausfiltern, Banken und Geldtransfer-Organisationen Warnhinweise bei entsprechenden Überweisungen aussprechen oder die Opfer selbst Verdacht schöpfen, wenn sie vom vermeintlichen Geliebten mit einer afrikanischen Vorwahl angerufen wurden. Heute nutzen die Betrüger diverse Tricks wie das Umleiten von IP-Adressen oder call-ID-spoofing (zur Verschleierung von Telefonnummern). Und für Geldtransfers wurden inzwischen von den Betrügern (teils mit unwissentlicher Hilfe durch Finanzagenten) in den Zielländern Konten angelegt und Mittelsmänner engagiert. Hinzu kommt, dass durch die Massenemigration, die ab den 1980er Jahren in Nigeria stattfand, eine weltweite Diaspora entstanden ist, die eine Art „human internet" (Ellis 2016, S. 165) bildet. Das bedeutet, dass die Online-Betrüger, die ja (derzeit) als Einzeltäter oder in kleinen Gruppen (also ohne übergreifende Organisationsstrukturen) operieren, Zugriff auf ein weltumspannendes soziales Netzwerk haben, von dem sie Informationen beziehen und auf das sie für die Abwicklung ihrer Betrügereien (etwa Geldwäsche, Finanztransfers etc.) zurückgreifen können. Dieses Netzwerk ist aufgrund der dort stattfindenden Kommunikation in regionalen Dialekten fast nicht überwachbar und aufgrund verwandtschaftlicher und ethnischer Bande kaum infiltrierbar. Wie die Entwicklung hier – und damit beim IRS – weiter verläuft, lässt sich schwer sagen. Es wird befürchtet, dass es zu einer zunehmenden Organisierung,

[23] So finden sich anstelle oder gemeinsam mit dem klassischen 419 scam Betrugsmaschen wie der CEO-Fraud, der Facebook Swindle, Heimarbeit-Betrug, der Hitman-Scam oder der Wash-wash-Scam.

24 Es gibt auf den ersten Blick ähnliche Maschen im Zusammenhang mit internationalen Partnervermittlungen (sog. „Katalogehen"). Gerade die „Russian Bride Scammer" erlangten um die Jahrtausendwende einige Popularität

Heubrock und Böttcher 2011. Bei einer genaueren Betrachtung zeigen sich allerdings deutliche Unterschiede zum IRS (hinsichtlich Täter, Opfer und modi operandi).

Zusammenarbeit und damit Professionalisierung der verschiedenen Gruppierungen kommt, mit der Folge, dass „enormous fraud rings“ (Rege 2009, S. 501) und ein arbeitsteilig differenzierter „underground market“ (Interpol und Trend Micro 2017, S. 4) entstehen. Dies würde eine zunehmende Verbesserung der zum Zweck der Täuschung eingesetzten Technologien und Vorgehensweisen nach sich ziehen – und damit ein noch stärkeres Gefährdungspotential.

Werfen wir einen kurzen Blick auf die anfangs angesprochene ‚Subkultur der Online-Betrüger‘. Internet-Betrug – das ist das Ergebnis etlicher ethnologischer Studien – hat in einigen (west-)afrikanischen Ländern mit der Zeit eine distinkte (Sub-)Kultur hervorgebracht (Cassiman 2018; Ellis 2016; Oduro-Frimpong 2011). Betrugspraktiken wurden in alte Glaubenssysteme von Magie und Aberglaube eingebettet und mit einer aggressiven Zurschaustellung des (illegal erworbenen) Vermögens sowie Referenzen auf Rap-Musik und -Modestil verschmolzen. Das ‚Scamming‘ ist in Westafrika also keineswegs eine nur Eingeweihten bekannte Tätigkeit, sondern ein bedeutsames popkulturelles Phänomen. Da sich die Selbstdarstellung der Scammer weitestgehend um „hot money“ dreht, also das (viele) betrügerisch erworbene Geld, das genauso schnell ausgegeben wie erlangt wird (Ellis 2016, S. 128), entwickeln sie eine gewisse Anziehungskraft auf Jugendliche. Gerade für (die häufig arbeitslosen) Universitätsabsolventen stellt dieser kriminelle Bereich inzwischen eine Karriereoption dar (Ojedokun und Eraye 2012)..

Beispiel Ghana: Bei den dortigen Romantikbetrügern (‚Sakawa Boys‘) handelt es sich um junge ghanaische Männer (zu 90 % unter 30 Jahren und meist undergraduate students), die in oder in der Nähe von urbanen Zentren wie Accra oder Kumasi (bzw. in den dortigen Slums wie Nima, Maamobi, Accra New Town oder Mallam Atta) leben. Sie sind oftmals arbeitslos und verbringen ihre Tage in Internetcafés (Warner 2011, S. 741). Diese sind nicht nur Orte jugendlicher Vergemeinschaftung, sondern teils auch Orte gemeinschaftlichen Betruges. Die sich selbst auch als „browsers“ (Cassiman 2018, S. 79) bezeichnenden Betrüger versuchen mit falschen Identitäten über Soziale Medien bzw. Online-Dating westliche Opfer – im dortigen Jargon als „paypal“ bezeichnet – zur Überweisung möglichst hoher Geldsummen zu bewegen. Sind dafür Telefonate erforderlich, greifen die „browsers“ auf entsprechende Komplizen („phone girls/boys“) zurück (Cassiman 2018, S. 81). Die erfolgreichsten Betrüger, ehrerbietig „hitter“ oder „barons“ genannt, nutzen ihr betrügerisch erworbenes Vermögen, um in bessere Viertel zu ziehen und sich dort mit einer Entourage an jungen, lernwilligen „browser“-Aspiranten zu umgeben. Die Anfänger in diesen Gruppierungen – „boy“ oder „maid“ genannt – müssen zunächst Hilfsarbeiten für ihren Master leisten, etwa Profilbilder beschaffen, IP-Adressen verschleiern, kleinere Chats übernehmen usw. (Cassiman 2018, S. 82). Die Tatsache, dass erfolgreiche „Barons“ betrügerisch große Vermögen erwerben und dies auch habituell nach außen hin demonstrieren, hat immensen Einfluss auf die Erwerbsaspirationen junger Afrikaner. Denn Online-Betrug ermöglicht (zumindest theoretisch) jedem, der bereit ist das ‚browsen‘ zu lernen und ein paar ghanaische Cedis für das Internetcafé hat, die Chance

auf einen schnellen sozialen Aufstieg. Die unmoralische Seite dieser Tätigkeit wird rationalisiert, indem das Scamming als ‚Revanche' für Jahrhunderte der Kolonisierung und Ausbeutung wahrgenommen wird (Warner 2011, S. 746).

Diese Sichtweise wird von vielen Landsleuten allerdings *nicht* geteilt. Bis hin in höchste Regierungskreise wird die Betätigung im Betrug als höchst unmoralisch gesehen, die Betrüger werden als faul, gierig und verdorben öffentlich gebrandmarkt. Und in der Tat hat die zunehmende Ausbreitung der Interkriminalität weitreichende gesellschaftliche Auswirkungen: Die vormals wirksamen Verteilungsmechanismen innerhalb der Gesellschaft erodieren – während einst Reiche ihre Verwandten, Freunden und Untergebenen an ihrem Vermögen teilhaben ließen, bleibt das betrügerisch erworbene Geld nun innerhalb kleiner krimineller Banden. Um Begehrlichkeiten zu entgehen, verlassen diese ihre angestammten Viertel und damit auch ihre ursprünglichen sozialen Beziehungen (Cassiman 2018, S. 84). In der Folge erodieren frühere Mechanismen von Loyalität und Freundschaft. Viele Betrüger haben qua ihres finanziellen Reichtums eine Vorbildfunktion, die sich auch auf die von ihnen vorgelebte Gier, Ichbezogenheit und Attitüde der ständigen Täuschung erstreckt. Dies wird auch von vielen Jugendlichen als ein moralischer Verfall empfunden. Auf der anderen Seite hat der Boom des Cybercrime Raub und Diebstahl in den Straßen von Nima deutlich verringert (Cassiman 2018, S. 84). Beachtlich ist außerdem, dass durch betrügerische Tätigkeiten gewonnenes Geld nicht mehr wie vormals benutzt wird, um ins Ausland zu reisen bzw. dorthin zu emigrieren. Stattdessen bleiben die Jugendlichen in Ghana, genießen dort den durch das Geld ermöglichten luxuriösen Lebensstil und demonstrieren diesen auch nach außen. All dies trägt dazu bei, dass der Romantikbetrug aller Voraussicht nach in Zukunft wohl eher zunehmen wird.

5. Die Geschädigten

5.1. Charakteristika

Oft stößt man beim IRS auf das Vorurteil, dass nur ein bestimmter ‚Typ Mensch' hier überhaupt zum Opfer werden kann. Die Studienlage zeichnet allerdings ein differenziertes Bild: Aufgrund seiner Variabilität kann der IRS unterschiedlichste Opfer ins Visier nehmen. Die Scammer können sich auf Alter, Geschlecht, Lebensumstände, sexuelle Orientierung usw. einstellen. Beispielsweise scheint es eine zunehmende Viktimisierung bei LGBT (engl. für Lesben, Schwule, Bisexuelle und Transgender) zu geben (Gillespie 2017, S. 219). Das derzeit typische Opfer des IRS ist allerdings eine Frau mittleren Alters – zumindest deuten (Hellfeld-)Statistiken und kriminalistische Lageeinschätzungen darauf hin. So hat das FBI festgestellt,

dass die erfassten Opfer von IRS zu 82 % weiblich und nur zu 18 % männlich waren[25]. Zu ähnlichen Ergebnissen kommt Whitty (2018) in ihrem aktuellen Überblick zu Charakteristika von IRS-Opfern. Neben dem Geschlecht spielt der Bildungsgrad eine Rolle, allerdings nur insofern, als dass Kenntnisse über Gefahren und Sicherheitsmaßnahmen im Internet die Wahrscheinlichkeit senken, Opfer eines derartigen Betrugs zu werden (Whitty 2018, S. 107)[26].

Nur wenige Studien befassen sich mit den *psychologischen Charakteristika* bzw. *Persönlichkeitsmerkmalen* der IRS-Opfer. Buchanan und Whitty (2014) testeten etwa verschiedene psychologische Items hinsichtlich ihrer Viktimisierungsrelevanz. Das Ergebnis: Nur wer in besonderem Maße an ‚Romantik' glaubt (erhöhter Grad des Items „Romantic Beliefs"), hat eine signifikant höhere Wahrscheinlichkeit zum Opfer zu werden. Ein Teilaspekt ist hier besonders relevant – der Glaube an die ‚Perfektheit' einer Beziehung („belief of idealization") (Buchanan und Whitty 2014, S. 273). Man kann sich vorstellen, dass eine Person mit derartigen Vorstellungen leicht Gefahr läuft, einen Scammer als etwas zu betrachten, was er nicht ist, dabei mögliche Warnsignale zu übersehen und so in eine ‚Beziehung' gezogen zu werden (Buchanan und Whitty 2014, S. 278). Allerdings ist die Aussagekraft beschränkt, da es sich hier nur um einen einzelnen psychologischen Faktor mit einer sehr niedrigen Effektstärke (Vorhersagekraft) handelt (Buchanan und Whitty 2014, S. 279).

In einer weiteren Studie prüft Whitty (2018) deswegen weitere Variablen, die IRS-Opfer kennzeichnen: Typische Opfer scheinen (mittelalte und höher gebildete) Frauen mit einem vergleichsweise hohen Grad an Impulsivität (hohe Werte bei Dringlichkeit und „Sensation Seeking") zu sein, was möglicherweise erklärt, warum sie so gut auf die dramatisierten Narrationen der Betrüger reagieren. Zudem verfügen sie über eine gewisse Sucht-Disposition – vielleicht fällt es ihnen deswegen so schwer, sich aus der Täuschung zu befreien (Whitty 2018, S. 108). Weiterhin zeichnen sich IRS-Opfer durch eine geringere Freundlichkeit („Kindness") aus. Vielleicht verfügen sie über kleinere Netzwerke oder dieser Wert ist ein Effekt des Betrugs selbst – in dem Sinne, dass der Betrüger das Opfer im Laufe der Täuschung in eine gewisse soziale Isolation gebracht und von seinen Netzwerken separiert hat (Whitty 2018, S. 108). Zu guter Letzt scheinen IRS-Opfer auch vergleichsweise vertrauensseliger als Nicht-Opfer zu sein. Keine dieser Variablen konnte jedoch die Viktimisierung durch den IRS hinreichend erklären. Insgesamt gilt also: IRS-Opfer lassen sich weder durch sozial-

[25] Bei derartigen Statistiken ist natürlich immer auch das Anzeigeverhalten unterschiedlicher Opfer zu berücksichtigen. Möglicherweise haben gerade Männer eine deutliche Hemmschwelle, solche ‚liebesbedingten' Betrugstaten zur Anzeige zu bringen.

26 Es ist also keineswegs so, dass niedrige Bildung die Viktimisierungswahrscheinlichkeit erhöht. Im Gegenteil, Studien deuten darauf hin, dass bei vielen Betrugsmaschen gilt: Je gebildeter eine Person ist, desto wahrscheinlicher ist es, dass sie zum Opfer wird. Möglicherweise führt Bildung zu einer gewissen Selbstüberschätzung (Fischer et al. 2013).

statistische noch durch psychologische Variablen zweifelsfrei charakterisieren – es gibt allenfalls Tendenzen.

5.2. Folgen

Ein IRS kann gravierende emotionale und psychische Folgen für Opfer haben – von Scham, Verlegenheit und Angst über Wut, Stress und Schock bis hin zu Depressionen, posttraumatischen Störungen und mitunter sogar Selbstmord. Viele Opfer geben sich selbst die Schuld (Whitty und Buchanan 2016, S. 186).

Besonders perfide am IRS ist, dass die Opfer mit der Aufdeckung des Betrugs einen zweifachen Schlag erleiden – sie verlieren ihr Geld und ihre (vermeintliche) Beziehung (Whitty 2018, S. 105). In einer Interview-Studie mit Opfern berichten diese von vielfältigen Auswirkungen (Whitty und Buchanan 2016): Ihr *emotionaler Zustand* nach dem Betrug ist äußerst negativ beeinflusst durch Gefühle von Scham, Ekel und Wut. Einige fühlen sich gewissermaßen sexuell missbraucht und vergewaltigt (Whitty und Buchanan 2016, S. 180). Die meisten (Männer wie Frauen) sind depressiv, manche suizidal. Hinzu kommt nicht selten eine *negative Reaktion des Umfelds*. Zentrale Personen im Leben des Opfers reagieren mit Unverständnis, sind teils wütend über den finanziellen Verlust (v.a. potentielle Erben), verweigern die so nötige Unterstützung und stigmatisieren die Opfer als dumm (Whitty und Buchanan 2016, S. 181). Aufgrund des massiven Geldverlustes leiden nicht wenige Opfer unter einer *Verschlechterung ihrer sozialen Situation* – der durch den Betrug bedingte finanzielle Ruin beschränkt ihre sozialen und lebensweltlichen Möglichkeiten enorm (Whitty und Buchanan 2016, S. 182). Am schwersten wiegt der Verlust der Beziehung. Der fiktive Partner wurde als ‚idealer Partner' erlebt. Für manche war die Beziehung regelrecht therapeutisch, in dem Sinne, dass sie sich ihrem Gegenüber vollends anvertrauen konnten, ohne Vorwürfe oder Kritik zu erfahren: „This relationship was so intense because they were able to self-disclose their inner most selves" (Whitty und Buchanan 2016, S. 183).

Dementsprechend finden es viele Opfer äußerst schwierig, den Kriminellen von seiner vorgetäuschten Identität zu separieren. Manchen ist die Beziehung so wichtig, dass sie auch weiterhin zahlen würden, nur um sie fortzusetzen. Andere begeben sich auf die Suche nach den wahren Personen hinter den gestohlenen Bildern oder versuchen sogar die Betrüger ausfindig zu machen (Whitty und Buchanan 2016, S. 182).

Im Hinblick auf mögliche Ent-Täuschungs- und Bewältigungsstrategien scheint eine Enthüllung signifikanten Anderen (Familie, Freunde, Bekannte) gegenüber zumeist nicht hilfreich, sondern eher schädlich zu sein. Denn seitens des sozialen Nahfeldes erfahren Opfer dieser unglaublich erscheinenden Masche statt Unterstützung häufig offen oder verdeckt geäußerte Vorwürfe und Unverständnis. Der Umgang mit der Polizei hingegen ist für viele Opfer regelrecht therapeutisch. Die Beamten zeigen in der Regel eine hilfreiche „unconditional positive regard" (Whitty und Buchanan 2016, S. 186). Ein Nebeneffekt dieser neutral-

empathischen Haltung kann allerdings sein, dass Opfer die Intentionen der Beamten missinterpretieren und sich in diese verlieben (‚transference effect'; vgl. Whitty und Buchanan 2016, S. 187)).

6. Psychologische und soziologische Erklärungsversuche

Retrospektiv erscheint der IRS sowohl den Opfern als auch äußeren Beobachtern unerklärlich. Wie ist es möglich, dass sich – obwohl zwischen Opfer und Täter niemals physischer Kontakt bestand – eine derart starke emotionale Bindung und suggestive Kraft besteht, dass große Vermögenswerte scheinbar ohne jegliche Zweifel und Vorbehalte übergeben werden?

Die psychologische und sozialpsychologische Forschung setzt sich intensiv mit Persuasion und Suggestion auseinander. Einige Arbeiten thematisieren dabei explizit den IRS und formulieren eine Reihe möglicher Erklärungen für dessen Wirksamkeit.

Neben den oben erwähnten psychologischen Merkmalen der Opfer werden hier v.a. die von den Betrügern verwendeten „persuasive techniques", die kognitive und motivationale Schwachstellen bei Entscheidungsprozessen ausnutzen, angeführt. Die entsprechenden Studien analysieren hierfür die initialen Scam-Mails (Carter 2015; Kich 2005), die Mail-Korrespondenzen zwischen Tätern und Opfern (Koon und Yoong 2013) oder deren Selbstbeschreibungen (Archer 2017). Das Ergebnis: Die Betrüger referieren den Autoren zufolge auf grundlegende Überzeugungsprinzipien (wie Reziprozität, Autorität, Sympathie, Knappheit etc.; etwa Archer 2017). Des Weiteren beruhe ihre Überzeugungskraft auf Kommunikationsstrategien zur Erzeugung von Glaubwürdigkeit – hierunter fällt beispielweise unmittelbare Befürchtungen ansprechen, auf dem Opfer Vertrautes/von ihm Geglaubtes zu referieren, dem Opfer eine Identität als Glückspilz o.ä. zuweisen (Carter 2015, S. 97), Sorge und Hingebung demonstrieren (Freiermuth 2011), Naivität/ Hilfsbedürftigkeit vorspiegeln oder sich (scheinbar) selbst offenbaren (Koon und Yoong 2013, S. 32). In diesen Zusammenhang gehört auch das Betonen moralischer und/oder religiöser Werte, etwa durch demonstratives Sprechen über den eigenen Glauben oder das Engagement in humanitären Organisationen (Kopp et al. 2017, S. 91).

Einen etwas anderen Ansatz verfolgt die Linguistin Konstanze Marx. Sie geht davon aus, dass die zentrale persuasive Strategie der Täter die der „kalkulierten Emotionskreation" (Marx 2012, S. 149) ist. Im Rahmen ihrer „linguistischen Persuasionsforschung" über Täter-E-Mails kommt sie zu folgendem Ergebnis (Marx 2012; Marx und Rüdiger 2017): Die wesentlichen Konstituenten einer Liebesbeziehung (Leidenschaft, Intimität, Verbindlichkeit) lassen sich auch über digitale Text-, Ton- und Bildbotschaften verwirklichen. Teilweise erscheinen solche reinen ‚Netz'-Beziehungen sogar noch intensiver, da auf den normalerweise durch körperliche Präsenz oder Alltagsprobleme besetzten Ebenen Projektionsflächen entste-

hen, die mit Wunschvorstellungen und Träumen aufgefüllt werden (Marx 2012, S. 150). Liebesbetrüger nutzen dies mittels einer „kalkulierten Emotionskreation“ aus, die auf drei Faktoren (Qualität, Intensität, Dauer) basiert. Hinsichtlich der „Qualität“ stellen sie sich als vertrauenswürdige Personen dar und bedienen dabei moralische wie geschlechtsspezifische Stereotype. „Intensität“ erzeugen sie nicht nur durch häufiges Kommunizieren, sondern auch durch die exzessive Verwendung von emotionsbezeichnenden und emotionsausdrückenden Wörtern (Kosenamen, Anredeformeln, Komplimente, Liebeserklärungen etc.) sowie einen höchst privaten Inhalt der Kommunikation (Erzählen des Alltags, Austauschen von Intimitäten usw.). Diese Korrespondenzen werden schließlich auf (eine gewisse) „Dauer“ gestellt, d.h. die Phase der Vertrauensetablierung umfasst mitunter bis zu ein Jahr, in dem hunderte, wenn nicht tausende Nachrichten ausgetauscht werden. Die Kontinuität und die schiere Menge der Informationen wirken sich vertrauensstabilisierend aus (Marx und Rüdiger 2017, S. 216). All dies zielt darauf, das Opfer in eine emotionale Falle zu locken. Diese Falle wird geplant und kalkuliert aufgebaut. Sie ist darauf ausgerichtet, das Opfer zu überzeugen, es gäbe jemanden, der tiefe Gefühle für es empfindet; gleichzeitig wird dem Opfer vermittelt, dass es auch ‚wert‘ sei, Adressat dieser Gefühle zu sein. Entsprechend wichtig und geschätzt ist der Täter für das Opfer und der Wunsch wächst, sich von Angesicht zu Angesicht zu sehen (Marx und Rüdiger 2017, S. 216). Wenn der Täter nun in eine scheinbar ausweglose Situation gerät, bleibt dem Opfer fast keine andere Möglichkeit, als ihm zu helfen.

Kopp (2016) greift auf einen anderen, mehr opferbezogenen Erklärungsansatz zurück. Für ihn beruht der Erfolg des IRS darauf, dass dieser auf tief verwurzelte erzählerische Deutungsrahmen zielt. Kopp bezieht sich dabei auf den Psychologen Robert J. Sternberg, nach dem jede Liebesbeziehung einer impliziten „story“ (Sternberg 1995) folgt. Jeder Mensch hat dezidierte, teils unbewusste Vorstellungen, wie Liebe sein sollte (Sucht, Kunst, Geschäft, Fantasie, Spiel, Herrschaft, Krieg usw.). Der Betrüger stellt sich also auf die Liebesgeschichte des Opfers ein und erschafft – je mehr Details das Opfer über sich preisgibt – eine immer passendere Geschichte. Das Kennenlernen ist so kein mitunter ernüchterndes Ersetzen von Fiktionen durch Fakten, wie das normalerweise geschieht, sondern ein geradezu rauschhaftes Bestätigen oder Übertreffen von Fiktionen, die in eine „ideale“ Liebesgeschichte münden (Kopp et al. 2015, S. 212). Das Opfer hat so (vom Täter beabsichtigt) das Gefühl, die Beziehung folge einem göttlichen/schicksalshaften Ablauf bzw. das Gegenüber sei der lange ersehnte „soul mate“ (Koon und Yoong 2013, S. 32). Der Betrüger „begin[s] to build an individual imagination of an ideal partnership“ (Kopp et al. 2016, S. 147). Nicht selten werden in die sich so entwickelnde Liebesgeschichte subtil Hinweise für spätere krisenhafte Wendungen eingeflochten, die dann als Basis für die nächsten Schritte des Betrugs fungieren (Kopp et al. 2015, S. 210). Dadurch bereitet er das Opfer unbemerkt auf die zu leistenden Geldzahlungen vor. Und nachdem diese erfolgt sind, baut er sie derart in die Beziehung ein, bis die Tätigkeit des ‚Geldschickens‘ zu einer normalen Aktivität wie Schreiben, Chatten oder Bilderschicken

geworden ist. Füllgrabe (2015) bezeichnet das als „psychologische Falle“, die ihre Wirksamkeit daraus gewinnt, dass die Betrüger den jeweiligen Bindungsstil und das Selbstkonzept ihres Opfers ausnützen.

Die Kriminalpsychologin Monica Whitty, die sich seit Jahren mit dem IRS befasst, beurteilt die meisten dieser Ansätze als mögliche, jedoch nicht hinreichende Erklärungen für die Überzeugungskraft des IRS (Whitty 2013). Ihrer Ansicht nach ergibt sich diese eher aus dem prozesshaften Aufbau des Betrugs. Dieses „Scammers Persuasive Technique Model“ führe dazu, dass die Opfer den Kommunikationsprozess mit dem Täter wie eine ‚Flow-Erfahrung‘ erleben, die sie immer mehr in den Bann dieser Beziehung hineinzieht und andere Interaktionen in ihrem Leben ausblenden lässt. „Victims described being caught up in the situation and in some ways immersing themselves into a world with the scammer“ (Whitty 2013, S. 679). Verstrickt in diese vom Täter induzierte Wirklichkeitskonstruktion akzeptieren die Opfer Whitty zufolge die ständigen Geldzahlungen unhinterfragt als Teil der Beziehung und sehen es nicht selten als Herausforderung, das viele Geld für den vermeintlichen Geliebten in Not zu besorgen (über Kredite, Freunde, Familie) und einen Weg zu finden, es diesem zukommen zu lassen. Manche Opfer seien erstaunlich findig darin, mögliche Schutzvorrichtungen (z.B. Überweisungssperren bei Banken oder Bargeldtransfersystemen wie Western Union) zu umgehen[27].

7. Präventionsmaßnahmen

Der IRS, wie er hier mit Blick auf bisherige internationale Forschungsergebnisse dargestellt wurde, erweist sich als komplexe, aber dennoch typische ‚Betrugsmasche‘, die zudem einem ständigen Formwandel unterliegt. Polizeiliche Ermittlungs- und Präventionsarbeit stehen dabei vor großen Schwierigkeiten. Derzeit laufen die meisten Ermittlungen beim IRS ins Leere – meist lassen sich aufgrund der Verschleierungsmöglichkeiten im Internet gar keine Täter identifizieren. Ist dies durch Zurückverfolgung der Kommunikation oder der Geldflüsse doch einmal möglich, so scheitern Festnahmen an der mangelnden internationalen Rechtshilfe mit den afrikanischen Ländern. In letzter Zeit ist es zwar – teils durch Zusammenarbeit mit Geschädigten – einige Male gelungen, Geldabholer bei der Übergabe zu verhaften. Diese spielen jedoch meist nur eine untergeordnete Rolle innerhalb der Betrügergruppierungen. In einigen anderen vom IRS betroffenen Ländern wurden deswegen verschiedenste Anstrengungen zur Bekämpfung des IRS bzw. der Cyberkriminalität insgesamt unternommen.

27 Wieso die Täter-Opfer-Kommunikation derart suggestiv ist, kann Whitty allerdings nicht vollends plausibel erklären. Was hier noch aussteht, sind empirische Analysen des konkreten Interaktionsgeschehens beim IRS. Der Autor dieses Beitrages bereitet derzeit entsprechende Analysen aus soziologischer Perspektive vor.

In *Großbritannien* beispielsweise gibt es seit einiger Zeit eine eigene Abteilung für Cyberkriminalität, die auch für den IRS zuständig ist. Diese Abteilung ist innerhalb der SOCA (Serious Organised Crime Agency) angesiedelt und setzt in der Bekämpfung des Romantikbetruges auf eine offensive Präventionstaktik. Diese beinhaltet sowohl das Informieren der Bevölkerung als auch die Erarbeitung von Gesetzen, die es erleichtern, potentielle Romantikbetrüger bei den Behörden zu melden, ohne als Organisation gegen Datenschutzbestimmungen zu verstoßen. In *Australien* wiederum werden opferorientierte Präventionsansätze getestet, bei denen „financial intelligence" von den australischen Behörden zur aktiven Bekämpfung von verschiedenen „online frauds", u.a. auch dem IRS, eingesetzt wurde (Cross 2016). Hierbei werden all jene identifiziert, die Geldüberweisungen in für den IRS typische Länder getätigt haben. Diese bekamen dann von den Polizeibehörden einen Brief übersandt, in dem vor einem möglichen Betrug gewarnt und Ansprechmöglichkeiten bei der Polizei genannt wurden. Die Evaluierung dieser Maßnahmen zeigte durchaus Erfolg und ein Großteil der Briefempfänger führte keine weiteren Geldtransfers durch. Der scheinbare Erfolg dieser Präventionsstrategie muss jedoch relativiert werden: Erstens muss nicht jeder Geldtransfer in eines der typischen IRS-Länder auch ein Betrug sein. Zweitens ist ungewiss, ob ein direkter Zusammenhang zwischen dem Brief und dem Einstellen der Zahlung besteht. Drittens ist die verfolgte Strategie mitnichten rein proaktiv, da schließlich mindestens eine finanzielle Transaktion bereits erfolgt sein muss. Und viertens sind Geldtransfers an Betrüger nicht auf einige typische westafrikanische Länder beschränkt. Es ist zu vermuten, dass auch die Täter zunehmend globaler agieren und/oder auf Finanzagenten im Inland zurückgreifen. Außerdem ist eine Überprüfung sämtlicher finanzieller Transaktionen ins Ausland logistisch für Ermittlungsbehörden nicht möglich und datenschutzrechtlich kritisch zu sehen.

8. Fazit

Das hier dargestellte Delikt des Romantikbetrugs mag im Kontext der Gesamtkriminalität gesehen eine eher marginale Rolle einnehmen. Gleichwohl verdeutlicht es exemplarisch einen wichtigen Punkt: Bei „Cybercrime" handelt es sich keineswegs immer um genuin neue Formen der Kriminalität, sondern es haben sich auch altbekannte Delikte (wie Diebstahl, Geldwäsche oder Pornographie) durch die Digitalisierung eine neue Plattform gesucht (Yar 2009). Dies gilt insbesondere für „alle erdenklichen modi operandi des Betrugs" (Priebe 2011). Grund dafür ist, dass das Internet es ermöglicht, die den ‚klassischen' Betrugsmaschen zugrundeliegenden, erprobten Täuschungsmanöver auf ein globales Level zu skalieren. Gleichzeitig haben sich verschiedene Teilaspekte des Betrugs, etwa die Suche nach oder das Ausspähen von passenden Opfern, durch Massenkommunikation und virtuelle Selbstdarstellung immens erleichtert, während die Strafverfolgung durch die Anonymität im Netz sowie der globalen, grenzüberschreitenden Online-Kommunikation kaum Möglichkeiten hat (Button et

al. 2014). Betrug und Täuschung werden so zu zentralen Herausforderungen in der Bekämpfung der Internetkriminalität, schließlich setzen sie an einem Punkt an, der sich nur sehr bedingt durch rechtliche Regelungen und technische Verfahren absichern lässt – den menschlichen Schwächen.

9. Literaturverzeichnis

Archer, Aaron K. (2017): "I Made a Choice": Exploring the Persuasion Tactics Used by Online Romance Scammers in Light of Cialdini's Compliance Principles. All Regis University Theses (823). Online verfügbar unter https://epublications.regis.edu/theses/823, zuletzt geprüft am 12.02.2018.

Aretz, Wera; Gansen-Ammann, Dominic-Nicolas; Mierke, Katja; Musiol, Annika (2017): Date me if you can. Ein systematischer Überblick über den aktuellen Forschungsstand von Online-Dating. In: *Z Sex-Forsch* 30 (01), S. 7–34. DOI: 10.1055/s-0043-101465.

Arora, Payal; Scheiber, Laura (2017): Slumdog romance. Facebook love and digital privacy at the margins. In: *MEDIA CULTURE & SOCIETY* 39 (3), S. 408–422. DOI: 10.1177/0163443717691225.

Boateng, Richard; Longe, Olumide; Stephen Isabalija, Robert; Budu, Joseph; Foundation Ghana, Pearlrichards (2011): Sakawa -Cybercrime and Criminality in Ghana. In: *Journal of Information Technology Impact* 11 (2), S. 85–100. Online verfügbar unter https://www.researchgate.net/publication/265446452_Sakawa_-Cybercrime_and_Criminality_in_Ghana, zuletzt geprüft am 30.04.2018.

Buchanan, Tom; Whitty, Monica T. (2014): The online dating romance scam: causes and consequences of victimhood. In: *Psychology, Crime and Law* 20 (3), S. 261–283. Online verfügbar unter http://www.scopus.com/inward/record.url?eid=2-s2.0-84893921823&partnerID=40&md5=883a89518bca17c153d83232b5864f98.

Button, Mark; Nicholls, Carol McNaughton; Kerr, Jane; Owen, Rachael (2014): Online frauds. Learning from victims why they fall for these scams. In: *Australian & New Zealand Journal of Criminology* 47 (3), S. 391–408. DOI: 10.1177/0004865814521224.

Carter, Elisabeth (2015): The anatomy of written scam communications. An empirical analysis. In: *Crime, Media, Culture* 11 (2), S. 89–103. DOI: 10.1177/1741659015572310.

Cassiman, Ann (2018): Browsers and phone girls. The intricate socialities of friendship, trust and cyberlove in Nima (Accra). In: *Africa* 88 (S1), S72-S89. DOI: 10.1017/S0001972017001152.

Cross, Cassandra (2016): Using financial intelligence to target online fraud victimisation. Applying a tertiary prevention perspective. In: *CRIMINAL JUSTICE STUDIES* 29 (2), S. 125–142. DOI: 10.1080/1478601X.2016.1170278.

Ellis, Stephen (2016): This present darkness. A history of Nigerian organised crime. London: Hurst & Company.

Freiermuth, Mark R. (2011): Text, lies and electronic bait: An analysis of email fraud and the decisions of the unsuspecting. In: *Discourse & Communication* 5 (2), S. 123–145. DOI: 10.1177/1750481310395448.

Füllgrabe, Uwe (2015): (Online-) Heiratsschwindel und andere Beziehungsfallen. In: *Kriminalistik* 69 (8-9), S. 487–493, zuletzt geprüft am 14.12.2017.

Gillespie, Alisdair A. (2017): The Electronic Spanish Prisoner. In: *The Journal of Criminal Law* 81 (3), S. 217–231. DOI: 10.1177/0022018317702803.

Heubrock, Dietmar; Böttcher, Max-Hendrik (2011): Scamming - Betrug durch vorgetäuschte Heiratsabsichten in Internet-Partnerschaftsportalen. In: *Kriminalistik* 65 (2), S. 75–81.

Interpol; Trend Micro (2017): Cybercrime in West Africa. Poised for an Underground Market. Online verfügbar unter https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-africa.pdf?_ga=2.124475466.1999533346.1525266343-1117850583.1525266343, zuletzt geprüft am 02.05.2018.

Kaufmann, Jean-Claude (2011): Sex@mour. Wie das Internet unser Liebesleben verändert. 1. Aufl. Konstanz: UVK.

Kich, Martin (2005): A Rhetorical Analysis of Fund-Transfer-Scam Solicitations. In: *Cercles* 14, S. 129–142, zuletzt geprüft am 22.02.2018.

Koon, Tan Hooi; Yoong, David (2013): Preying on lonely hearts. A systematic deconstruction of an Internet romance scammer's online lover persona. In: *Journal of Modern Languages* 23 (1), S. 28–40, zuletzt geprüft am 21.02.2018.

Kopp, Christian (2016): Structural analysis of Online Romance Scams by applying the transtheoretical model in conjunction with the theory of personal love stories. Federation University Australia. Online verfügbar unter https://library.federation.edu.au/record=b2687776, zuletzt geprüft am 12.02.2018.

Kopp, Christian; Layton, Robert; Sillitoe, Jim; Gondal, Iqbal (2015): The Role of Love stories in Romance Scams: A Qualitative Analysis of Fraudulent Profiles. In: *International Journal of Cyber Criminology; ISSN: 0974 – 2891* 9 (9), S. 205–217, zuletzt geprüft am 12.02.2018.

Kopp, Christian; Sillitoe, James; Gondal, Iqbal (2017): “I am your perfect online partner". Analysis of Dating Profiles Used in Cybercrime. In: *APJABSS* 3 (2). DOI: 10.25275/apjabssv3i2ss5.

Kopp, Christian; Sillitoe, James; Gondal, Iqbal; Layton, Robert (2016): The Online Romance Scam: A Complex Two-Layer Scam. In: *Journal of Psychological and Educational Research* 24 (2), S. 144–161.

Marx, Konstanze (2012): Liebesbetrug 2.0 - Wie emotionale Illusionen sprachlich kreiert werden. In: Marina Iakushevich und Astrid Arning (Hg.): Strategien persuasiver Kommunikation. Hamburg: Dr. Kovač (Schriftenreihe Philologia, 168), S. 147–165.

Marx, Konstanze; Rüdiger, Thomas-Gabriel (2017): Romancescamming. Eine kriminologisch-linguistische Betrachtung. In: *Kriminalistik* 71 (4), S. 211–218.

Oduro-Frimpong, Joseph (2011): Sakawa: On Occultic Rituals and Cyberfraud in Ghanaian Popular Cinema. Working paper presented to the Media Anthropology Network e-seminar European Association of Social Anthropologists, 18 Jan- 1 Feb 2011. Online verfügbar unter http://www.media-anthropology.net/file/frimpong_rituals_cyberfraud.pdf, zuletzt geprüft am 12.04.2018.

Oduro-Frimpong, Joseph (2014): Sakawa Rituals and Cyberfraud in Ghanaian Popular Video Movies. In: *African Studies Review* 57 (02), S. 131–147. DOI: 10.1017/asr.2014.51.

Ojedokun, Usman Adekunle; Eraye, Michael Christopher (2012): Socioeconomic Lifestyles of the Yahoo-Boys: A Study of Perceptions of University Students in Nigeria. In: *International Journal of Cyber Criminology; ISSN: 0974 – 2891* 6 (2), S. 1001–1013.

Rege, Aunshul (2009): What’s Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud. In: *International Journal of Cyber Criminology; ISSN: 0974 – 2891* 3 (2), S. 494–512. Online verfügbar unter http://www.cybercrimejournal.com/AunshulIJCCJuly2009.pdf, zuletzt geprüft am 16.05.2013.

Rüdiger, Thomas-Gabriel (2012): Cybergrooming in virtuellen Welten – Chancen für Sexualtäter? In: *Deutsche Polizei. Zeitschrift der Gewerkschaft der Polizei* 61 (2), S. 29–35.

Schwartz, Victoria (2015): Wie meine Internet-Liebe zum Albtraum wurde. Das Phänomen Realfakes. 2. Auflage. München: Blanvalet.

Sternberg, Robert J. (1995): Love as a Story. In: *Journal of Social and Personal Relationships* 12 (4), S. 541–546. DOI: 10.1177/0265407595124007.

Toma, Catalina L. (2017): Developing online deception literacy while looking for love. In: *MEDIA CULTURE & SOCIETY* 39 (3), S. 423–428. DOI: 10.1177/0163443716681660.

Walther, Joseph B. (1996): Computer-Mediated Communication. In: *Communication Research* 23 (3), S. 3–43. DOI: 10.1177/009365096023001001.

Warner, Jason (2011): Understanding Cyber-Crime in Ghana: A View from Below. In: *International Journal of Cyber Criminology; ISSN: 0974 – 2891* 5 (1), S. 736–749. Online verfügbar unter http://cybercrimejournal.com/warner2011ijcc.pdf, zuletzt geprüft am 30.04.2018.

Whitty, Monica T. (2013): The Scammers Persuasive Techniques Model. Development of a Stage Model to Explain the Online Dating Romance Scam. In: *British Journal of Criminology* 53 (4), S. 665–684. Online verfügbar unter doi:10.1093/bjc/atz009.

Whitty, Monica T. (2015): Anatomy of the online dating romance scam. In: *SECURITY JOURNAL* 28 (4), S. 443–455. DOI: 10.1057/sj.2012.57.

Whitty, Monica T. (2018): Do You Love Me? Psychological Characteristics of Romance Scam Victims. In: *Cyberpsychology, behavior and social networking* 21 (2), S. 105–109. DOI: 10.1089/cyber.2016.0729.

Whitty, Monica T.; Buchanan, Tom (2012): The online romance scam. A serious cybercrime. In: *Cyberpsychology, behavior and social networking* 15 (3), S. 181–183. DOI: 10.1089/cyber.2011.0352.

Whitty, Monica T.; Buchanan, Tom (2016): The online dating romance scam. The psychological impact on victims - both financial and non-financial. In: *CRIMINOLOGY & CRIMINAL JUSTICE* 16 (2), S. 176–194. DOI: 10.1177/1748895815603773.

Zillmann, Doreen; Schmitz, Andreas; Blossfeld, Hans-Peter (2011): Lügner haben kurze Beine. Zum Zusammenhang unwahrer Selbstdarstellung und partnerschaftlicher Chancen im Online-Dating. In: *Zeitschrift für Familienforschung* 23 (3), S. 291–318.